Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 54 (2015) 47 – 56

Procedia Computer Science

Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)

Contriving Hybrid DESCAST Algorithm for Cloud Security

Nandita Sengupta* and Ramya Chinnasamy

University College of Bahrain, Information Technology Department, Manama, Bahrain

Abstract

Cloud computing has taken a major part in IT industry both for an individual and the organization. Primarily, it's used as infrastructure as a service, platform as a service, file storage, disaster recovery and backup. In cloud computing, protection of data in server and while in media is a challenging issue. Our proposed encryption algorithm Hybrid DESCAST has been designed to provide the security of huge volume of data sent through the media and the same will remain encrypted in the cloud sever. This cipher text will be decrypted only when the same is required to be used by the authenticated user. Problems of individual DES and CAST Block Cipher Algorithm have been tackled by our proposed encryption algorithm. Complexity and Computation time for encryption and decryption for our proposed algorithm is higher than the individual DES and CAST algorithm. This paper is focused to provide security of data in cloud server, as well as for the data while transferring from client to cloud server and vice versa.

Peer-review under responsibility of organizing committee of the Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)

Keywords: Block cipher algorithm; Cloud security; Encryption algorithm; Hybrid DESCAST.

1. Introduction

Using Internet Technologies, Cloud Computing is contributing a lot in the industries. Also as an individual, people are using cloud computing because of its enormous benefits. Capital expenditure has been reduced substantially and flexibility of execution of the business processes have changed the scenario of the industries. The could computing has provided many facilities, like Infrastructure as a Service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS), Disaster Recovery, Backup to the industries which made the cloud popular. Hence, there is no option for thinking whether cloud computing will be adopted or not. Importance should be given to the point when the use of cloud computing should be started. IT-enabled business services are being delivered by Cloud computing in exponential manner. Dynamically scalable, virtualized computing environment can be achieved by adopting cloud technology with affordable cost and resources. Scalable IT resources like IT hardware, software, expertise and infrastructure management can be available on demand by cloud technology which are otherwise exorbitant. Location independent or device independent processes, applications and services can be available on demand. The organizations can make use of resources on demand without maintaining it because the cloud provider is responsible for the environment.[1–4]

*Corresponding author. Tel.: +973-17794412; fax: +973-17793828.
E-mail address: [a]ngupta@ucb.edu.bh

Peer-review under responsibility of organizing committee of the Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)
doi:10.1016/j.procs.2015.06.006

2. Motivation

Cloud computing is open pervasive systems connected by heterogeneous networks in the distributed environment, which makes security a big gainsay. Organizations that are moving from the traditional standalone environment to the cloud are having great concern about the cloud security. The cloud provider has to offer more security of data to the cloud consumer to improve the trust. As the cloud technology is improving day by day encryption associated with cloud computing should also be advanced. Discerning the working principle of cloud encryption is the key to understanding the security of the cloud. To increase the level of security various cryptographic algorithms have been used. Block and stream cipher algorithms are the most commonly used algorithms each with its pros and cons. This paper proposes a hybrid DESCAST algorithm that combines DES and CAST block cipher algorithms to improve the data protection and information security.[5]

3. Contribution

Since Security is a great concern for many organizations for cloud adoption, cloud providers have to provide more protection of data and information in storage and transfer. In this paper, we propose a hybrid DESCAST algorithm that will increase the level of security of data by avoiding the disadvantages of individual algorithms. This algorithm utilizes the same space as single DES or CAST algorithm with advanced security.

4. Literature Review

Confidentiality, integrity and availability for client's systems and datasets can be enforced by changing the security controls from legacy perimeter and detection-based tools to a focus on implementing increased protection at the application and data levels. Data access controls can start with categorizing data and be implemented by denying or allowing access based on multiple requirements like user id, multi-form factor authentication, type of device, application set, time of day and location. There has been an increased number of sophisticated strikes for critical financial and user data. This has cost many companies billions of dollars and loyalty loss. Cloud encounters recent high-profile attacks that compromised end-points such as teller registers, end-user laptops and payment terminals and perpetrates malicious activities. There is a real vulnerability across industries which are using cloud services. There has been a real and growing challenge of inadequate protection or an improperly used devices as the world is expecting quintuple number of connected devices by 2020. Extreme focus should be given to security of the cloud provider's SPI(Software as a service, Platform as a service, Infrastructure as a service) when sensitive data stored in the cloud. In order to reduce the initial cost, many cloud-based solutions have been developed by small teams with inadequate security knowledge which poses serious security vulnerability and threat to the cloud environment. It is very difficult to find out when user credentials have been stolen or compromised in the Cloud environments which makes it weak access logging and access authentication, in turn making it far harder to detect malicious intruder. Organizations want the benefits of cloud computing such as cost-effectiveness ,scalability and flexibility. But they can't afford to lose control of their data. The data has to be protected while transferring and at storage in cloud.Data 'at rest' should also be encrypted because there is a chance of stealing of data 'at rest'. The inactive data which is stored on the cloud, is called as data 'at rest'.

4.1 Security challenges in SaaS model

Typically applications in SaaS are delivered to cloud consumer via the Internet through a Web browser. But, weakness in web applications may generate vulnerabilities for the SaaS applications. Attackers are using the web to compromise user's computers and do malicious activities. Traditional security solutions do not effectively protect attacks on SaaS, even though the same challenges as that of any web application technology occurs. We need to devise new approach for security in SaaS cloud computing model. Since the same database stores data from multiple tenants, there is a great chance of data leakage between tenants. In SaaS, cloud customer has to rely on provider for data security which is a major challenge. In the case of disaster, the data needs to be recovered which in turn needs

backup of data. This introduces additional level of security concern. Cloud provider has to encrypt the backup data also. Applications can be accessed over the internet via web browser from any computer or mobile devices. This in turn imposes additional security threat.

4.2 Security challenges in PaaS model

As with other cloud computing models, PaaS also relies on reliable and secure network and secure web browser. PaaS provides traditional programming languages and third party web service components. Hence PaaS inherits security issues related to third party web services. In the case of application development, developers are responsible for building secure applications that may be hosted on the cloud. The system development life cycle and security will be affected by the speed at which applications will change in the cloud. In order to ensure flexibility to keep up changes, the developers must ensure that the PaaS applications should be upgraded frequently. This in turn affects security. data legal issues should be known comprehensively to the developers to ensure that data is stored in appropriate locations. Data may be stored in different places with different legal regimes which in turn affect security and privacy. In PaaS, providers are responsible for securing the underlying infrastructure as well as the applications services since developers do not usually have access to the underlying layers. If there is weakness in the development environment tools provided by a PaaS provider, then it will also affect the security of applications developed by the developer. PaaS offers development tools to create SaaS applications and both of them may use multi-tenant architecture. The cloud provider is responsible for security of data while in transfer, process and storage.

4.3 Security challenges in IaaS model

Plenty of resources such as network, storage, servers and other computing resources have been provided by the IaaS through a network usually internet. Cloud provider controls the network and storage which in turn makes them responsible for security of those resources. Cloud consumers have complete hold of software resources which in turn makes them responsible for the security of those resources. Virtual machines can be created by the users through the concept of virtualization which adds additional layers to the underlying structure. This additional layer makes it vulnerable to security breaches. Since virtual machines have physical and virtual boundary, it adds greater challenge to security. Virtual machine isolation is done by virtual machine manager or hypervisor. If there is a security breach in VMM, then virtual machine is also under threat. For maintenance, load balancing and fault tolerance, the virtual machine is migrated across physical servers. Virtual machines on the same server shares resources like CPU, storage and Input/output of the server which degrades the security. If there is one malicious virtual machine using the shared resources, then that VM may intrudes other virtual machine also. There is a prepackaged software template called virtual machine image repository which gives configuration files to create virtual machines (VM). Cloud consumers can use the template provided by the VM image repository or can create one of their own. A malicious intruder may change the VM image repository by using the any security vulnerability and can compromise other virtual machine users. If there is an error, then virtual machines can roll back to their previous states.This may introduces additional security issues such as deactivated malicious intruder gains access again. The virtual machine should be copied before rollback which introduces accrued vulnerabilities. Virtual machine changes their states such as on, off or suspended when moving through environment. Virtual machines that are in off may use malicious VM image repository for on which is a serious threat.

4.4 Most common security challenges in cloud computing

There are lot of security threats to cloud computing. A single fault in one client application could allow an intruder to gain access to more than one client's data. This problem is known as data breaches. A malicious hacker may delete entire data in the cloud if there is a vulnerability in cloud provider side. This is known as data loss. If a hacker gains access to client's credentials, then he can eavesdrop on client's activities and transactions and may redirect clients to illicit sites. This is known as service traffic hijacking. Weak interfaces and APIs can exhibit serious security issues to data like confidentiality, integrity, availability, and accountability. This is known as insecure interfaces and APIs. A DoS (Denial of service) attack occurs when the hacker can able to temporarily or indefinitely interrupt or suspend

cloud services. A malicious insider is a hacker who can gain access to the cloud data, system and network and do illicit activities. A malicious insider can be a current or former employee or a business contractor. Cloud abuse occurs when a hacker gains access to cloud service and disseminate malware, or share pirated software. Insufficient due diligence occurs when cloud development team is insufficiently familiar with cloud technologies. Since the cloud provider has to share infrastructure, platform and application, there is a chance of shared technology vulnerability. When an intruder tampers the secret key stored in a cryptographic hardware device and observes the result of the cryptographic primitive under modified secret key, then a related-key attack (RKA) is said to occur. When the intruder has access to both the plaintext, and cipher text, then the known-plaintext attack (KPA) is said to occur. A cryptanalytic attack, where the attacker consistently checks all possible keys until the correct one is found is known is a brute-force attack. The practical feasibility of a brute-force attack is influenced by the key length. Shorter keys are more vulnerable than the longer one.

4.5 Other security issues in cloud computing

Cloud providers should perform background screening of their employees. Lack of employee screening and poor hiring practice makes the cloud vulnerable to malicious insider attack. Normally anyone who has valid credit card and email can open account in cloud without checking the credentials of the customers. With lack of background screening of cloud consumers, a malicious tenant may intrude to other cloud consumers resources. Peoples should be educated about security, lack of which degenerates security. Many technologies like web services, web browsers and virtualization has been used by cloud computing. Any weakness in technology affect the security of the cloud[6–10].

5. Importance of Cloud Security

Flexibility and cost effectiveness are the main pulling factor towards cloud computing models[11–14]. Certain challenges should be addressed by cloud computing to make as sustainable option to traditional data services. The major challenge is the issue of security. Data integrity and privacy can be harder to maintain because of the externalized aspect of outsourcing. It also affects support, data, service availability, demonstrate compliance, and security access to applications and information. In short, added level of risk must be confronted in cloud computing. Trust relationships between cloud computing providers and the organizations which are using cloud should be accomplished. Organizations should realize real risk in terms of how these providers implement, deploy, and manage security[15,16]. The security risks in all kind of services should be addressed by cloud provider[4]. Various levels of IT risk is present in each type of cloud computing model—public, private or hybrid. As private cloud is possessed and managed by a single organization, cloud owner does not share resources with any other company. On the other hand, in public clouds, cloud providers provide IT activities and functions as a service which can be billed on a pay-per-use or subscription basis via the Internet. All the resources are owned by cloud provider in the case of public cloud, Which provides sharing of IT resources in a multitenant environment which in turn improve utilization rates with abbreviated cost while maintaining access to high quality technology. But this possess high level of security risk.

6. Cipher Algorithms

A cipher algorithm is a mathematical formula contrived specifically to hide the content of data and information transmitted over a network. Key is a primary matter in many major cipher algorithm. Data or information is encrypted with the key and the same key or complementary key is needed to decrypt the data or information back. Encryption is the process of converting a plaintext message into an obscure message called cipher text[17,18]. The reverse process of decoding data that has been encrypted is known as decryption. An encryption algorithm along with a key is used in the process of encrypting message. Decryption algorithm which works with the same key used for encryption is called symmetric key algorithm. There are different types of data encryption and encryption standards. Encryption schemes are based on block or stream ciphers.

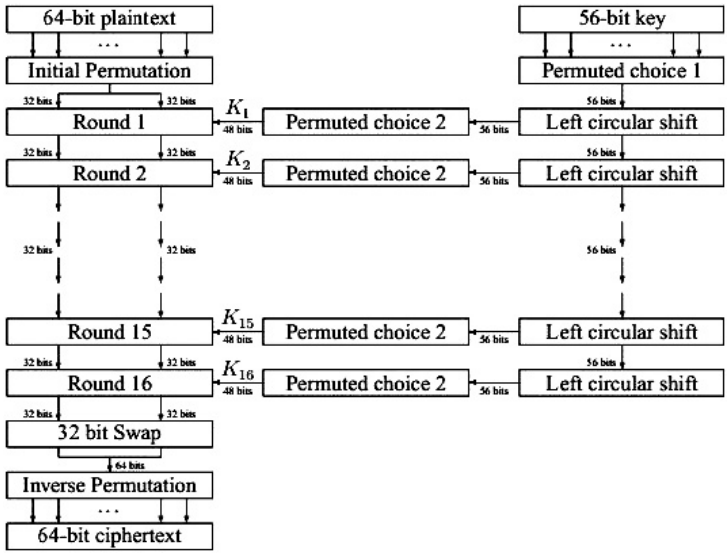

Fig. 1. Flow diagram for DES.

6.1 Block-cipher algorithm

A symmetric key cipher algorithm which is operating on fixed-length groups of bits, called blocks, is known as block cipher algorithm. A block cipher encryption algorithm might take fixed length block of plaintext as an input, and output a cipher text of fixed length block of same size. The exact transformation is controlled using a second input — the secret key. Similarly in decryption, a fixed length block of cipher text together with the secret key, yields the original fixed length block of plaintext. A message longer than the block size can be decomposed into number of blocks of fixed length and each block is encrypted with secret key of some size using block cipher algorithm. Following are some examples of block cipher algorithm.

6.1.1 DES algorithm

DES (Data Encryption Standard) is block cipher algorithm designed at IBM and is based on a cipher known as the Feistel block cipher. It has number of rounds in which each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. The plaintext to be encrypted and the secret key is given as input to the DES. Since DES uses same secret key for both encryption and decryption, it is a symmetric key algorithm. It is a 64 bit block cipher as it only operates on 64 bit blocks of data at a time. Key is also considered as 64 bit and least significant bit of each byte is used as parity check. Therefore, 56 out of 64 bits are used as input key for permutation and further processing. The plain-text message which needs to be encrypted, is arranged into 64 bit blocks. The last block will be padded with random character, if the number of bits in the message is not evenly divisible by 64. Multiple permutations and substitutions are included to increase the difficulty of performing a cryptanalysis on the cipher. Flow diagram of DES Algorithm[19] has been illustrated in Fig. 1.

Advantages

- There has been no known weakness to DES since it's inception (since 1977).
- It was an official United States Government standard;
- As DES is an ANSI and ISO standard, anyone can implement it with any programming language.
- DES is fast in hardware and relatively fast in software.

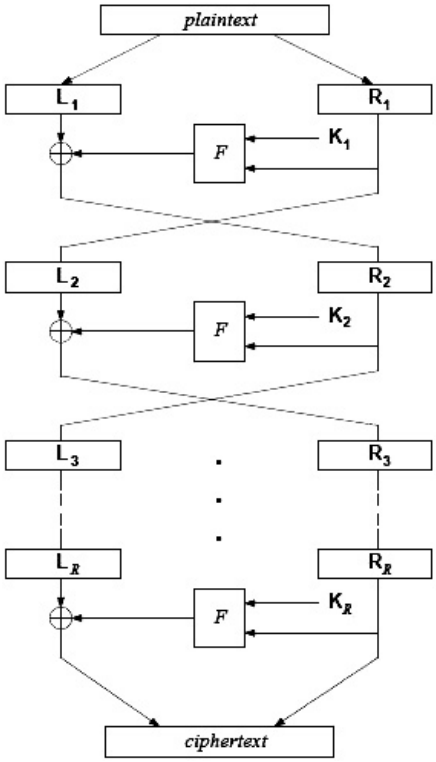

Fig. 2. Flow diagram for CAST.

Disadvantages

- DES was not designed for software and hence runs relatively slowly.
- With advancement in cryptanalysis, brute force attack is possible on DES.

Triple DES is an extension of DES algorithm Where the DES algorithm is applied three times in sequence with three different keys. The key size is thus 168 bits (3 times 56), which in turn makes the algorithm robust against brute-force techniques. But this algorithm is relatively vulnerable to attack via birthday problem with it's three 56 bit keys.

6.1.2 CAST algorithm

The CAST encryption algorithm is symmetric key block cipher algorithm. It is framed with substitution boxes (S-boxes) with fewer input bits than output bits. The CAST algorithm accomplishes "confusion" and "diffusion" principles through series of rounds of substitutions. H. M. Heys *et al.*, illustrates the basic algorithm as shown in Fig. 2^{20}. In the CAST^{21} algorithm the N-bit plaintext input block is split into two halves. The right half block, R1, along with the Key K1 are transformed by a round function F and then XORed bit-by-bit to the left half-block, L1. The resultant of this process are then swapped with R1. This process is iterated for the number of rounds in the cipher, R. Accordingly, the algorithm may be viewed as the following repeated operation:

$$R_{i+1} = F(R_i, K_i) \oplus L_i$$
$$L_{i+1} = R_i$$

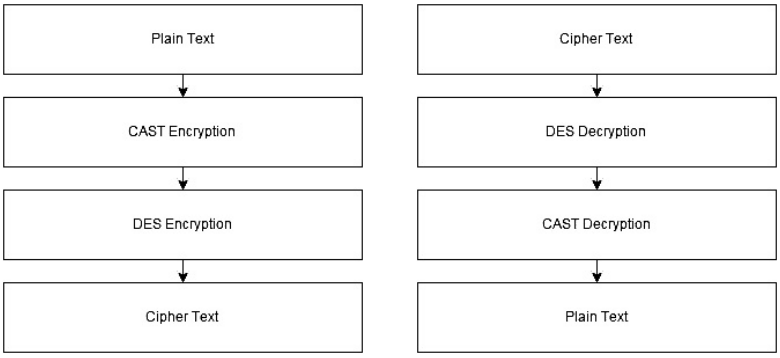

Fig. 3. (a) Encryption; (b) Decryption.

6.2 Block-cipher algorithm challenges

In block cipher method, all blocks are encrypted with the same key and because of that security is degenerated. Cipher text gets repeated whenever plain text gets repeated.

7. Proposed Hybrid DESCAST Algorithm

To overcome the security challenges, we propose an algorithm which combines both CAST and DES cipher algorithm. There are 2 phases of encryption. In the first phase, CAST encryption algorithm is applied to plain text. In the second phase DES encryption algorithm is applied to the encrypted text. The pictorial representation of encryption algorithm is illustrated in Fig. 3(a). Similarly, Decryption process has 2 phases. In the first phase, DES decryption is applied to the cipher text. In the second phase, CAST decryption is applied to the decrypted text. Fig. 3(b) gives the pictorial representation of decryption process.

8. Experimental Results

We have used Python3.4 and it's pycrypto package for implementing the proposed algorithm. Small input data, "This is my sample input string" has been considered for getting experimental results. Key for CAST algorithm is 128 bits (b'Sixteen byte key') and key for DES algorithm is 64 bits ('01234567'). Output after "CAST", Hybrid DESCAST encryption are shown in Fig. 4. Also, output after decryption, DES and CAST are shown in Fig. 4.

```
>>> ================================ RESTART ================================
>>>
Cipher text for the plain text
This is my sample input string
using CAST algorithm is    :
b'\xeb\xb9\x07w\t\xc4\xff\xe7&\\\xe9$\x14\xba\xc2\x8c\x1e\x9bn\xc3\xbd8\xa3\xf1\x97U\x0b\x17\xf1\xac\xc4\xf1'

Cipher text for the plaintext
This is my sample input string
 using DESCAST algorithm is
b'\x95\x85v2,B4|\xa3\xa4\xbf\x0e\x80i\xaf\xbc\xe7\xba\\\x16Y2_\xabF%\xe1{\x14y\n*'

decrypted Cipher text for the phase1 is
b'\xeb\xb9\x07w\t\xc4\xff\xe7&\\\xe9$\x14\xba\xc2\x8c\x1e\x9bn\xc3\xbd8\xa3\xf1\x97U\x0b\x17\xf1\xac\xc4\xf1'

decrypted ciphertext using DESCAST is
This is my sample input string
>>>
```

Fig. 4. Sample output.

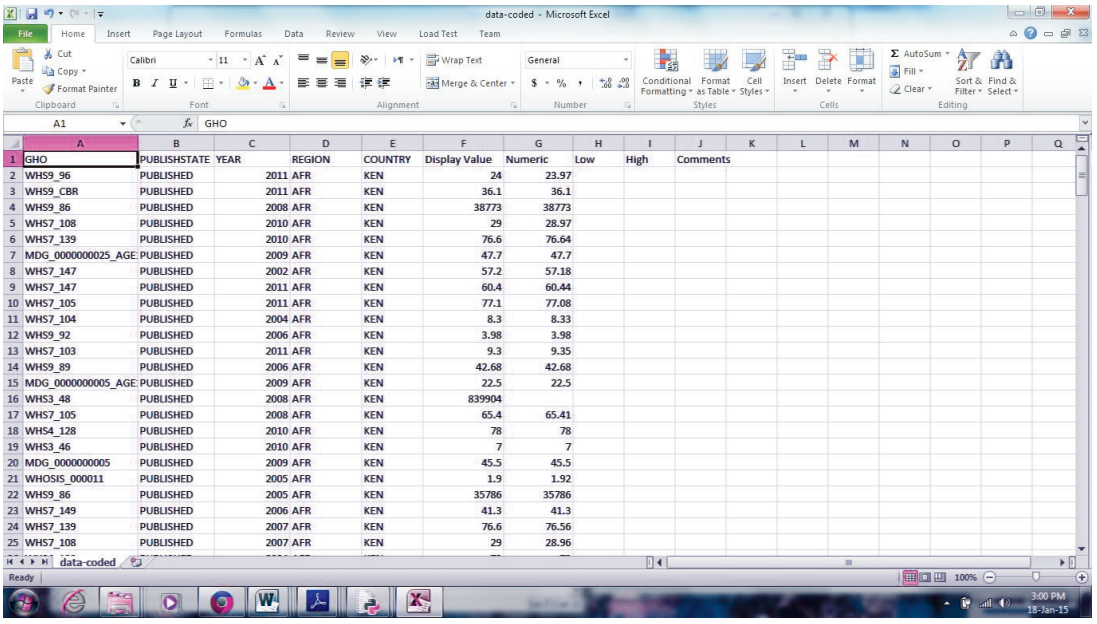

Fig. 5. Plain text input file (data-coded.csv).

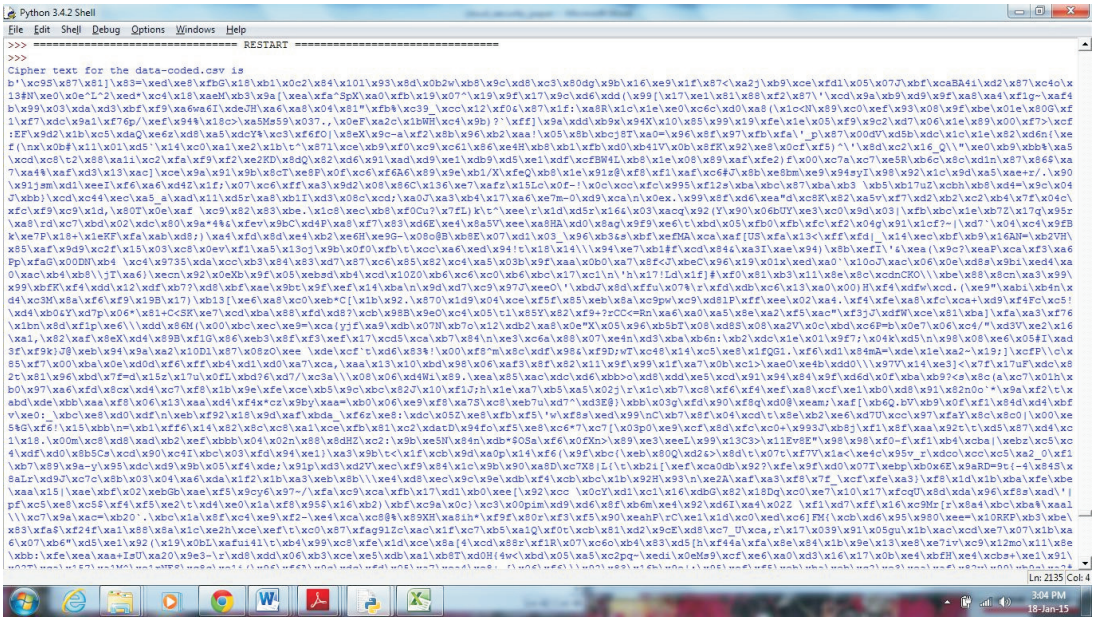

Fig. 6. Cipher text output.

Economic data of a country from world bank (data-coded.csv) has been taken as plain text input[22] which is shown in Fig. 5. Encrypted output, i.e., cipher text output of this high volume of data is represented in Fig. 6. We have used system with 6 GB RAM and 2.50 GHz processor for implementing and testing the proposed algorithm.

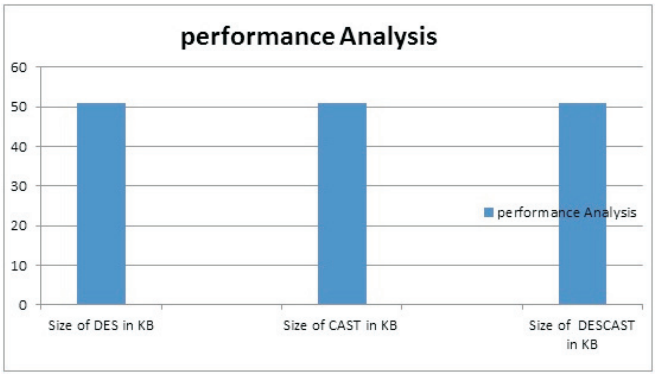

Fig. 7. Performance analysis.

9. Performance Analysis

Performance of DES and CAST are same when applying individually. In case of CAST algorithm, differential related key attack is possible. DES offers better performance with half of the memory occupied, when compared to other symmetric key block cipher algorithms such as MARS, IDEA and RC6. When combining CAST and DES algorithms, the possibility of linear cryptanalysis using known plain text attack and related key attack has been averted. The hybrid algorithm is more secure than individual algorithm[23]. The size of the cipher text of plaintext using DESCAST algorithm is same as that of individual DES or CAST algorithm. So we can achieve more protection with the same space. The analysis of space utilized by each algorithm is given in Fig. 7.

10. Conclusion

By combining 128 bit key and 64 bit key cipher algorithms, the brute-force attack and attacks via birthday problems were averted and the algorithm is more robust. The implemented DESCAST algorithm can be applied to any kind of data with size less than 1 MB. We have tested the DESCAST algorithm on data from worldbank[22], Standard & Poor's 500[24], Organization of the Petroleum Exporting Countries (OPEC)[25] and World health organization[26]. This algorithm can be applied in 3G and 4 G LTE environments. The DESCAST algorithm is relatively slow on big data.

11. Future Work

Improve the performance of the algorithm so that it can be applied on big data in 5 G LTE environment for cloud security.

References

[1] J. Xiong, X. Liu, Z. Yao, J. Ma, Q. Li, K. Geng and S. P. Chen, A Secure Data Self-Destructing Scheme in Cloud Computing. *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 448–458, October–December 1 (2014).
[2] P. Jamshidi, A. Ahmad and C. Pahl, Cloud Migration Research: A Systematic Review, *IEEE Transactions on Cloud Computing*, vol. 1, no. 2, pp. 142–157, July–December (2013).
[3] M. Ficco and M. Rak, Stealthy Denial of Service Strategy in Cloud Computing, *IEEE Transactions on Cloud Computing*, vol. 3, no. 1, pp. 80–94, January–March 1 (2015).
[4] Y. Zhang, X. Liao, H. Jin and G. Min, Resisting Skew-Accumulation for Time-Stepped Applications in the Cloud via Exploiting Parallelism, *IEEE Transactions on Cloud Computing*, vol. 3, no. 1, pp. 54–65, January–March 1 (2015).
[5] A. C. Chen, M. Won, R. Stoleru and G. G. Xie, Energy-Efficient Fault-Tolerant Data Storage and Processing in Mobile Cloud, *IEEE Transactions on Cloud Computing*, vol. 3, no. 1, pp. 28–41, January–March 1 (2015).
[6] Thomas Erl, P. Ricardo and M. Zaigham, Cloud Computing: Concepts, Technology & Architecture, Prentice Hall.
[7] S. Roschke, C. Feng and C. Meinel, Intrusion Detection in the Cloud, Dependable, Autonomic and Secure Computing, 2009. DASC'09, *Eighth IEEE International Conference*, E-ISBN: 978-1-4244-5421-1, pp. 729–734, December (2009).

[8] K. P. Shelke, S. Sontakke and D. A. Gawande, Intrusion Detection System for Cloud Computing, *International Journal of Scientific & Technology Research*, vol. 1, issue 4, ISSN 2277-8616, May (2012).
[9] IBM, Security and High Availability in Cloud Computing Environments, *IBM Global Technology Services Technical White Paper*, June (2011).
[10] K. Hashizume, G. D. Rosado, F. E. Medina and B. E. Fernandez, An Analysis of Security Issues for Cloud Computing, *Journal of Internet Services and Applications*, 4:5, doi:10.1186/1869-0238-4-5, (2013).
[11] D. Zissis and D. Lekkas, Future Generation Computer Systems, *ELSEVIER The International Journal of Grid Computing and eScience*, vol. 28, pp. 583–592, (2012).
[12] N. P. Smart, Algorithms, Key Size and Parameters Report – 2014. *European Union Agency for Network and Information Security*, (2014).
[13] T. Olufon, C. E-A Campbell, S. Hole, K. Radhakrishnan and A. Sedigh, Mitigating External Threats in Wireless Local Area Networks, *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 6, no. 3, December (2014).
[14] P. R. Padhy, R. M. Patra and C. S. Satapathy, Cloud Computing: Security Issues and Research Challenges, *IRACST – International Journal of Computer Science and Information Technology & Security (IJCSITS)*, vol. 1, no. 2, December (2011).
[15] F. Ayoub and K. Singh, Cryptographic Techniques and Network Security, *Communications, Radar and Signal Processing, IEE Proceedings F*, vol. 131, issue 7, November (2008).
[16] P. Schoo, V. Fusenig, V. Souza, M. Melo, P. Murray, H. Debar, H. Medhioub and D. Zeghlache, Challenges for Cloud Networking Security, HP Laboratories.
[17] H. Gilbert, Design and Analysis of Cryptographic Algorithms for Mobile Communication Systems, Orange Labs.
[18] P. D'Avilar, J. D'Errico, K. Berends and M. Peck, Authenticated Encryption, *https://www.cs.jhu.edu*.
[19] *www.facweb.iitkgp.ernet.in/∼sourav/DES.pdf*
[20] H. M. Heys and E. S. Tavares, On the Security of the CAST Encryption Algorithm, Queen's University, Kingston, Ontario, Canada.
[21] J. Nakahara Jr and M. Rasmussen, Linear Analysis of Reduced-round CAST-128 and CAST-256, UNISANTOS, Brazil, LSI-TEC, PKI Certification Department.
[22] *http://data.worldbank.org/country*
[23] A. M. Mushtaque, Comparative Analysis on Different Parameters of Encryption Algorithms for Information Security, *JCSE International Journal of Computer Science*, vol. 2, issue 4, E-ISSN:2347-2693.
[24] *http://finance.yahoo.com/q/hp?s=%5EGSPC+Historical+Prices*
[25] *http://www.opec.org/opec_web/en/publications/338.htm*
[26] *http://www.who.int/research/en/*